SUMÁRIO

1. INTRODUÇÃO

Ataques à infraestrutura estratégica de um país, espionagem industrial e internacional, fraudes bancárias e uso militar do espaço cibernético – esses eventos, e muitos outros que têm ocorrido e continuarão a ocorrer diariamente, levantam questões importantes sobre o papel e a responsabilidade dos Estados em relação a incidentes cibernéticos. Os Estados devem exercer o controle soberano sobre a infraestrutura cibernética que se localiza em seu território? Se assim for, os Estados têm a responsabilidade de controlar as atividades cibernéticas que emanam ou as que apenas trafegam através de seus ativos cibernéticos? Em outras palavras, até que ponto um Estado tem que controlar as atividades de atores não estatais, tais como ativistas cibernéticos, organizações criminosas e terroristas, quando essas ações cibernéticas podem causar danos a outras pessoas ou Estados?

A resposta a estas perguntas orbita em grande parte em torno da doutrina de soberania no direito internacional. Na medida em que as nações exercem a sua soberania sobre o espaço cibernético e sua infraestrutura, isto fornecerá respostas-chave para o nível de controle que os Estados devem exercer e quanta responsabilidade estes devem aceitar quando não conseguirem fazê-lo adequadamente, ao falhar em deter atividades cibernéticas ilegais.

Assumiremos que os Estados têm poder soberano sobre a sua infraestrutura cibernética e que com esse poder vem a responsabilidade de controlá-la e impedir que ela seja conscientemente utilizada para perpetrar atividades prejudiciais a outros Estados e indivíduos. Esta responsabilidade, de evitar atividades cibernéticas ilegais, estende-se não apenas aos agentes estatais, mas também para os intervenientes não estatais. Este poder soberano e a responsabilidade que dele advém, enquanto quase exclusiva, necessariamente possuem algumas limitações.

Na área emergente de operações cibernéticas, a aplicação da doutrina de soberania para atividades neste espaço criou um controverso debate entre Estados, acadêmicos e especialistas. O Manual Tallinn reflete algumas das controvérsias sobre o princípio da soberania aplicado ao espaço cibernético, sugerindo que os Estados estão hesitantes, atualmente, em aceitar a responsabilidade pelas atividades cibernéticas que se originam em seu território. No caso dos ataques cibernéticos que atingiram a Estônia em 2007, a Rússia não só negou qualquer responsabilidade como também recusou as solicitações por parte da

Estônia para que investigasse e extraditasse os potenciais cri- minosos que agiram de dentro do território russo. No caso do *malware* “Stuxnet”, apesar de inúmeras alegações e evidências de que os Estados Unidos e Israel estavam diretamente envolvidos, nenhum dos dois países admitiu oficialmente qualquer responsabilidade ou participação neste caso. Esta hesitação, por parte dos Estados, em aceitar a responsabilidade por incidentes que ocorrem através da Internet é o produto de duas grandes questões inerentes à estrutura desta: a dificuldade de atribuir de maneira oportuna a responsabilidade de um ataque (levando em consideração os mecanismos de ocultação na rede) e o método randômico em que os dados trafegam pela infraestrutura cibernética, normalmente levando o caminho de menor resistência, sem respeito à geografia.

Esta dificuldade inerente à atribuição faz com que os Estados permaneçam cautelosos em aceitar responsabilidade por ataques originados de seu território, não só porque eles não podem identificar o atacante em tempo hábil, mas porque, mesmo se pudessem identificar o computador a partir do qual se origina o ciberataque, é improvável que eles saibam quem está por trás do computador. Da mesma forma o anonimato permite ao Estado adotar medidas moralmente questionáveis, sabendo que a atribuição de responsabilidade é praticamente impossível. Isto é especialmente verdadeiro para as medidas tomadas por diversos países através de *proxies*, como atores não estatais, a fim de atingir objetivos políticos, militares ou econômicos.

2. O CONCEITO DE SOBERANIA TERRITORIAL

Independentemente das várias teorias sobre a função legal do território, é de ampla aceitação que, segundo o princípio da soberania territorial, um Estado exerce completa e exclusiva autoridade sobre o seu território. Max Huber, na arbitragem “Ilhas Palmas”, afirmou esse princípio geral da seguinte forma: “Soberania nas relações entre os Estados significa independência. Independência em relação a uma porção do globo é o direito de exercer nela, à exclusividade de quaisquer outros Estados, as funções de um Estado.” (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1928). De acordo com o Tribunal Internacional de Justiça: “Entre Estados independentes o respeito à soberania territorial é um fundamento essencial das relações internacionais.” (1952, apud DAHLHOFF, 2012, p.35). Além disso, o Estado tem o

direito de controlar o acesso e a saída do seu território; este pressuposto parece aplicar-se também a todas as for- mas de comunicação. A soberania territorial protege um Estado contra qualquer forma de interferência por parte de outros Estados. Enquanto tal interferência pode implicar a utilização da força, esse aspecto não é tratado no presente artigo.

Deve-se ter em mente que a soberania territorial não se limita somente à garantia de proteção aos Estados, mas também impõe obrigações aos mesmos, especialmente a obrigação de proteger no seu território os direitos de outros Estados, nomeadamente o seu direito à integridade e à inviolabilidade em paz e em guerra, juntamente com os direitos que cada Estado pode reivindicar sobre seus nacionais em território estrangeiro.

A Corte Internacional de Justiça, na sua decisão “Canal de Corfu”, confirmou este entendimento de soberania: “por soberania, entendemos todo o conjunto de direitos e atributos que um Estado possui em seu território, com a exclusão de todos os outros Estados, e também nas suas relações com outros Estados” (CIJ, 1949). Apesar de o poder soberano de um Estado ser quase absoluto, ele é limitado por certos princípios do direito internacional, incluindo as ações do Conselho de Segurança das Nações Unidas, o Direito Internacional dos Conflitos Armados e os direitos humanos fundamentais. Há também áreas onde, com base no acordo consensual e costume, nenhum Estado pode afirmar a soberania, como o alto-mar. Essa área tem sido tratada como *res communis*, o que significa que ela pertence a toda comunidade internacional e não pode ser apropriada por nenhum Estado. Existem outras áreas onde os atores estatais concordaram em soberania não exclusiva, como a Antártica, o fundo do mar e a lua. Estas são áreas onde nenhum Estado exerce o poder, mas onde todos os compartilham o poder, com base em acordo.

3. SOBERANIA TERRITORIAL E ESPAÇO CIBERNÉTICO

Espaço cibernético tem sido definido como um domínio global dentro do ambiente da informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computadores incorporados, processadores e controladores. É um termo taquigráfico que se refere ao ambiente criado pela confluência de redes cooperativas de computadores, sistemas de informação e infraestruturas de telecomunicações, comumente referido como a *World Wide*

Web. É verdade que o ciberespaço é caracterizado pelo anonimato e pela onipresença, por isso parece lógico assimilá-lo ao alto-mar, espaço aéreo internacional e espaço sideral, ou seja, a considerá-lo um *global common* ou legalmente um *omnium res communis*. No entanto, essas caracterizações apenas justificam a conclusão óbvia de que o espaço cibernético, em sua totalidade, não está sujeito à soberania de um Estado ou de um grupo de Estados. Dadas as suas características, é imune a apropriação.

Apesar da classificação correta de "espaço cibernético como tal" como uma prática *res communis*, o ciberespaço, ou melhor, os seus componentes físicos, não são imunes à soberania e ao exercício da jurisdição. Por um lado, os Estados têm exercido, e continuarão a exercer, a sua jurisdição penal *vis-à-vis* a crimes cibernéticos e continuarão a regular as atividades no ciberespaço. Por outro lado, é importante ter em mente que o ciberespaço exige uma arquitetura física para existir. O equipamento respectivo geralmente está localizado no território de um Estado. É de propriedade do governo, de empresas ou de pessoas físicas. Ele é conectado à rede elétrica nacional. A integração dos componentes físicos, ou seja, a infraestrutura cibernética localizada no território de um Estado, para o "domínio global" do ciberespaço, não pode ser interpretada como uma renúncia ao exercício da soberania territorial, não impedindo um Estado de exercer a sua soberania, especialmente a sua jurisdição penal, à infraestrutura cibernética localizada em áreas cobertas pela sua soberania territorial.

Os Estados têm continuamente enfatizado o seu direito de exercer controle sobre a infraestrutura cibernética localizada nos seus respectivos territórios, a fim de exercer a sua jurisdição sobre as atividades cibernéticas no seu território e proteger sua infraestrutura cibernética contra qualquer interferência transfronteiriça perpetrada por outros Estados ou indivíduos.

É preciso enfatizar que a aplicabilidade do princípio da soberania para os referidos componentes e atividades no ciberespaço não é barrada pelo caráter inovador e original da tecnologia subjacente. Isso vale para a maioria das normas e princípios do direito internacional consuetudinário que se aplicam ao ciberespaço e às atividades cibernéticas. O presidente dos Estados Unidos da América (THE WHITE HOUSE, 2011, p.9), no âmbito da Estratégia Internacional para o Ciberespaço de 2011, afirmou claramente que o

> "desenvolvimento de normas para a conduta do Estado no

> ciberespaço não exige uma reinvenção do direito internacional costumeiro, nem impossibilita normas internacionais existentes. As normas internacionais de longa data que orientam o comportamento do Estado – em tempos de paz e conflito – também se aplicam no ciberespaço".

Isso não significa necessariamente que as referidas regras e princípios são aplicáveis ao ciberespaço em sua interpretação tradicional. Tendo em vista o caráter novo do ciberespaço e tendo em conta a vulnerabilidade da infraestrutura cibernética, há uma incerteza perceptível entre os governos e juristas se as normas e princípios do direito internacional consuetudinário tradicionais são suficientemente aptos a fornecer as respostas desejadas a algumas questões preocupantes. É, portanto, de extrema importância que os Estados não só concordem com a aplicação do direito internacional consuetudinário ao ciberespaço, mas também sobre uma interpretação comum que leve em devida consideração as características únicas da tecnologia de rede. Por isso, é necessário que os governos continuem a trabalhar de maneira cooperativa para criar um consenso a respeito de normas de comportamento aplicáveis ao ciberespaço.

4. APLICABILIDADE DA SOBERANIA TERRITORIAL NO ESPAÇO CIBERNÉTICO

A aplicabilidade do princípio da soberania territorial ao ciberespaço implica que a infraestrutura cibernética localizada no território terrestre, nas águas interiores, no mar territorial, e, quando aplicável, nas águas arquipelágicas ou no espaço aéreo nacional está coberta pela soberania territorial do respectivo Estado. Assim, a princípio, o Estado tem o direito de exercer o controle sobre essas infraestruturas e atividades cibernéticas nessas áreas. Não pode ser deixado fora de consideração, no entanto, que o exercício da soberania pode ser restringido por normas consuetudinárias ou convencionais do direito internacional, tais como a imunidade de correspondência diplomática ou os direitos de passagem inofensiva, passagem em trânsito e rotas marítimas arquipelágicas.

A primeira consequência do que foi inferido acima é que a infraestrutura cibernética localizada em áreas sob a soberania territorial está protegida contra a interferência externa. Esta proteção não está limitada às atividades que caracterizam uma utilização injustificada de

força, um ataque armado ou uma intervenção ilegal. É importante notar que nem todos os Estados concordam plenamente que os impactos sobre a infraestrutura cibernética de outro Estado constitui, necessariamente, uma violação do princípio da soberania territorial. Ressalta-se que, se o resultado de atos de interferência infligem danos materiais à infraestrutura cibernética localizada em outro Estado, parece haver um consenso suficiente de que tal ato constitui uma violação da soberania territorial do Estado agredido. Neste contexto, é preciso reconhecer que, segundo alguns, o dano infligido deve ser grave. Se, no entanto, não há danos materiais relevantes à infraestrutura cibernética, não é entendido consensualmente se essa atividade pode ser considerada uma violação da soberania territorial. O exemplo usual dado é espionagem, incluindo espionagem cibernética, porque o direito internacional carece de uma proibição das atividades de espionagem.

De acordo com a Estratégia Internacional para o Ciberespaço dos EUA, as seguintes atividades podem qualificar-se como violações da soberania territorial: ataques às redes e sua utilização para atos hostis que ameaçam a paz e a estabilidade, as liberdades civis e a privacidade. Enquanto os respectivos atos não são especificados, infere-se que o governo dos EUA está se resguardando para uma aplicação mais ampla e incisiva do princípio da soberania territorial, porque afirma o direito de responder a tais atos com todos os meios necessários, incluindo, se necessário, o uso convencional da força. No que diz respeito a infraestrutura cibernética, protegida assim pelo princípio da soberania territorial, é irrelevante se ela pertence ou é operada por instituições governamentais, entidades privadas ou pessoas físicas.

Deve-se ter em mente, no entanto, que no caso de um conflito armado o princípio da imunidade sobera- na não desempenha nenhum papel nas relações entre os Estados beligerantes. Em seguida, os objetos que gozam de imunidade soberana podem ser destruídos (caso se qualifiquem como alvos legítimos) ou estar sujeitos à apreensão pelas forças armadas inimigas. Além disso, a imunidade soberana não é ilimitada. Por exemplo, a aeronave remotamente pilotada Lockheed Martin RQ-170, de propriedade dos EUA foi interceptada e forçada a pousar pelo Irã (alegadamente por meio cibernéticos) em 2011, estava sobrevoando o espaço aéreo nacional iraniano e, assim, violou a soberania territorial deste. Assim, o Irã tinha o direito de utilizar todos os meios necessários, incluindo meios cibernéticos, para deter essa violação de sua soberania.

À luz do exposto acima, podemos afirmar que a soberania territorial possui um relevante peso

legal e de grande eficácia no direito internacional; tal princípio pode ser aplicado ao ciberespaço sem modificações de largo escopo se este é entendido como compreendendo componentes físicos – ou infraestrutura cibernética – que estão localizados no território de um Estado ou de outro modo protegido pelo princípio da soberania territorial. Contudo, esta conclusão não implica que todos os aspectos de proteção da soberania territorial foram esclarecidos. Por exemplo, ainda não há um consenso entre os Estados a respeito de quais operações cibernéticas se qualificam como uma utilização imprópria da força, de acordo com o artigo 2 da Carta da ONU, ou como uma agressão armada ao abrigo do artigo 51. As referências bastante abstratas para infraestruturas críticas não são muito úteis se não há consenso a respeito de que objetos e instituições estão sendo considerados críticos.

Igualmente eficaz é o conceito de jurisdição territorial. Por conseguinte, os Estados têm o direito de regular as atividades cibernéticas que ocorrem nos seus territórios e fazer valer o seu direito interno. Embora os Estados gozem de um direito quase ilimitado de exercer a sua jurisdição territorial, em relação às atividades e infraestruturas cibernéticas nos seus territórios, há uma necessidade indiscutível de uma compreensão acordada internacionalmente de que a funcionalidade e os benefícios da *internet* serão seriamente ameaçados se os Estados não exercerem a sua jurisdição territorial com respeito pelas redes de outras nações e pelo espaço cibernético como um todo. Finalmente, os governos também devem cooperar entre si a fim de melhorar as suas capacidades na área da ciência forense cibernética. Tais esforços de cooperação são necessários não só para identificar os atacantes, mas também para a dissuasão mais eficaz dos Estados e atores não estatais com intenções de uso maléfico do espaço cibernético

5. O ESPAÇO CIBERNÉTICO E A ESTRATÉGIA DE DEFESA BRASILEIRA

No Brasil, a segurança e a defesa do espaço cibernético é um assunto recente e de baixa visibilidade. Assim, não se tem como dimensionar o grau de conectividade e interdependência dos equipamentos e sistemas de informação e muito menos da conectividade e interdependência das infraestruturas críticas, tais como redes de esgoto, rede de distribuição de água, redes de telefonia e redes de operação e distribuição de energia. Caso estas redes e sistemas forem interrompidos ou destruídos, provocarão um impacto político, econômico e

social na sociedade de tal ordem que podem pôr em risco a segurança nacional. Por isto, são de suma importância estudos sobre a defesa do espaço cibernético.

Inclusive, em setembro de 2013, a Agência de Segurança Nacional dos Estados Unidos (NSA) monitorou o conteúdo de telefonemas, e-mails e mensagens de celular da ex-presidente Dilma Rousseff e de um número indefinido de "assessores-chave" do governo brasileiro.

A Agência Brasileira de Inteligência (Abin) confirmou uma ameaça ao Brasil publicada em novembro de 2015 em conta no Twitter vinculada a um membro do Estado Islâmico (EI) e intensificou o monitoramento de indivíduos que teriam jurado lealdade ao grupo extremista e poderiam agir dentro do País em virtude dos Jogos Olímpicos.

O Centro Integrado Antiterrorismo (Ciant) fez um monitoramento nos pedidos de credenciamento para a Olimpíada. Eles descobriram que 40 pessoas estão com alertas a respeito de cooperação internacional, sendo que quatro delas tinham ligação comprovada com o terrorismo.

Na área governamental, a defesa cibernética foi tratada, inicialmente, com o desenvolvimento da Segurança da Informação, o que se caracterizou com a criação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001, que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998. Ao novo órgão, dentre outras competências, coube à coordenação das atividades de Segurança da Informação.

Na Política Nacional de Defesa é citado por diversas vezes a importância da segurança no espaço cibernético. Além de ressaltar a importância de minimizar a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento.

Pelo Decreto nº 5.772, de 8 de maio de 2006, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no GSI/PR, com a missão de planejar e coordenar a execução das atividades de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal (APF). Em dezembro de 2008, a Estratégia Nacional de Defesa (END) estabeleceu prioridade em três setores estratégicos para a Defesa Nacional: Nuclear, Cibernético e Espacial.

A Estratégia Nacional de Defesa, sobre o setor cibernético diz:

“No setor cibernético, as capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. As prioridades são as seguintes:

(a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;

(b) Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à cerificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;

(c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;

(d) Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;

(e) Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;

(f) Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos: operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;

(g) Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e

(h) Estruturar a produção de conhecimento oriundo da fonte cibernética.”

A Diretriz Ministerial nº 0014, de 2009 do Ministério da Defesa, de 9 de novembro de 2009, definiu providências para o cumprimento da END nos setores estratégicos da defesa, estabelecendo as responsabilidades para cada Força Armada.

O Setor Cibernético é citado no Livro Branco de Defesa Nacional como:

"A ameaça cibernética tornou-se uma preocupação por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional. A proteção do espaço cibernético abrange um grande número de áreas, como a capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede. O Setor possui elementos intra e interorganizacionais; é multidisciplinar e gera produtos e serviços tecnológicos diversos, além de métodos e processos gerenciais em todos os níveis. A implantação do Setor Cibernético tem como propósito conferir: confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em suas redes, os quais são processados e armazenados. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas de ciência e tecnologia e operacional. Sob a coordenação do Exército, significativos avanços têm se concretizado na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico. Assim, foram estabelecidas as seguintes premissas para o projeto:

- contemplar multidisciplinaridade e dualidade das aplicações;
- fomentar a base industrial de defesa;
- induzir a indústria nacional a produzir sistemas inovadores; e
- produzir componentes críticos nacionais.

O Centro de Defesa Cibernética do Exército vem somar esforços com as organizações governamentais já existentes, e busca:

- melhoria da capacitação dos recursos humanos;
- atualização doutrinária;
- fortalecimento da segurança;
- respostas a incidentes de redes;
- incorporação de lições aprendidas; e
- proteção contra ataques cibernéticos."

6. A DEFESA DA SOBERANIA TERRITORIAL BRASILEIRA NO ESPAÇO CIBERNÉTICO

Com a virada do milênio e com os novos avanços da tecnologia militar em um momento pós Guerra-Fria, o espaço cibernético se dimensiona como uma nova zona de conflito e recebe cada vez mais a atenção das autoridades de todo o mundo. Em virtude disso, atualizações nos documentos que possuem as principais diretrizes para a defesa da soberania brasileira se fizeram necessárias, ocasionando, por exemplo, na concepção da Estratégia Nacional de Defesa (Decreto n° 6.703, 18 de dezembro de 2008) que define como setores estratégicos da Defesa : o nuclear, o cibernético e o espacial.

A Defesa Cibernética é definida por "conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente." (EME, Brasília, 2010)

Tendo em vista essa necessidade em defesa cibernética, o Exército assume o papel principal dentro das Forças Armadas Brasileiras, no que tange a desenvolvimento e pesquisa da área, bem como na proteção de órgãos militares e governamentais. Assim, criou-se o Comando de Comunicações e Guerra Eletrônica do Exército (CCOMGEX), organizações militares subordinadas a esse comando (CIGE, ES COM, 1° BGE, BA ADM e CIA C²), Instituto Militar de Engenharia e Centro de Defesa Cibernética (CDCIBER), que ocupa papel principal nessa função de defesa.

O CDCIBER, também subordinado ao Ministério da Defesa nas Operações Conjuntas é constituído de um Estado-Maior conjunto na realização do planejamento e controle das ações planejadas, considerando as características de cada força armada buscando a sinergia entre as mesmas. O Centro ainda é classificado como o órgão central O Sistema Militar E Defesa Cibernética atuando em cinco principais áreas: Doutrina, Operações, Inteligência, Ciência e Tecnologia e Capacitação de Recursos Humanos. É importante frisar, como umas os principais meios de garantia de segurança do espaço cibernético, a capacitação dos oficiais e sargentos em Guerra Cibernética, estágios de Defesa Cibernética aos Cadetes da AMAN e salientar a importância da sua atuação na condução de grandes eventos como a Rio +20, Jornada Mundial da Juventude, Copa do Mundo e Copa das Confederações.

De acordo com a Portaria Normativa Nº 2.777/MD, de 27 de outubro de 2014 as medidas para o fortalecimento da Defesa Cibernética nacional se dividem entre o Estado-Maior Conjunto das Forças Armadas (EMCFA), que se torna supervisor e adoção de medidas como a criação do Comando de Defesa Cibernética e da Escola Nacional de Defesa Cibernética, a Secretaria-Geral do Ministério da Defesa, encarregada das providências relativas à disponibilização de recursos orçamentários para os projetos em andamento, propostas de criação de infraestruturas de apoio e do enquadramento das tecnologias do setor cibernético nas prioridades do Ministério da Defesa. Além dos órgãos ligados ao âmbito estratégico temos o Exército Brasileiro, em articulação com o EMCFA, encarregado a tomada e providências para a imediata ativação e inicio os trabalhos do Comando de Defesa Cibernética e da Escola Nacional de Defesa Cibernética e pela organização e execução dos projetos de Defesa Cibernética com ênfase para os seguintes pontos: implantação e consolidação do desenvolvimento conjunto de Defesa Cibernética, implantação e consolidação o Sistema de homologação, certificação de produtos de Defesa Cibernética, apoio a pesquisa e desenvolvimento de produtos de Defesa Cibernética e a criação do Observatório de Defesa Cibernética.

Na Marinha do Brasil (MB) a defesa cibernética começou na década de 90 e veio se aperfeiçoando com o tempo. Mesmo que as pesquisas e desenvolvimentos nessa área sejam de responsabilidade do Exército, a Marinha possui estudos e alguns avanços nesse sentido. A MB trabalha em três frentes na defesa cibernética: pessoas, com cursos, palestras, etc ; processos, normatizando e estabelecendo procedimentos; e tecnologias, com implementações de redes seguras, firewall, além de softwares e outros programas que previnem e defendem ataques cibernéticos. Por isso, a Marinha em sua doutrina de DC contempla alguns principios, estabelece ações, busca a capacitação do pessoal, dentre outros assuntos. Com isso, são feitas simulações de DC para que se mantenha o treinamento do pessoal com um alto padrão de excelência, em ambientes controlados simulando cenários de defesa e análise de vírus. Assim, a Marinha do Brasil trabalha para estar preparada e, se necessário for, defender a sociedade de possíveis ataques cibernéticos.

7. CONSIDERAÇÕES FINAIS

Tendo em vista a segurança cibernética como fator diferencial no novo cenário mundial e observando os casos que podem vir a comprometer a segurança nacional brasileira, o espaço

cibernético tem recebido cada vez mais atenção do governo, que tem tomado diversas medidas em prol de garantir a defesa cibernética da nação. Tais medidas já foram regulamentadas em diversos documentos, porém ainda necessitam de tempo para suas realizações plenas. O Exército Brasileiro já iniciou seus trabalhos em grandes eventos, entretanto, ainda é necessário um maior desenvolvimento tecnológico para que se evite uma quebra de soberania do território nacional através do espaço cibernético.

REFERÊNCIAS BIBLIOGRÁFICAS

FERREIRA, Carlos. **Pela defesa do espaço cibernético brasileiro: panorama mundial e nacional**. Disponível em: http://www.desenvolvimentistas.com.br/blog/carlosferreira/2013/02/28/pela-defesa-do-espaco-cibernetico-brasileiro-panorama-mundial-e-nacional/ Acesso em 17 de mai. 2017.

DAHLHOFF, Guenther. International Court of Justice: Digest of Judgments and Advisory Opinions, Canon and Case Law 1946-2012. Londres: Brill, 2012.

DE CARVALHO, Paulo Sergio M. **A Defesa Cibernética e as Infraestruturas Críticas Nacionais.** Disponível em: www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf

Estratégia Nacional de Defesa. Disponível em: http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em 17 mai. 2017.

HEINEGG, Wolff. Legal Implications of Territorial Sovereignty in Cyberspace, NATO Cooperative Cyber Defence Centre of Excellence (2012). Disponível em: . Acesso em: 19 de jul. 2016.

JENSEN, Eric. Cyber Sovereignty: The Way Ahead, Texas International Law Journal (2015). Disponível em: . Acesso: em 25 jul. 2016.

KANUCK, Sean. Sovereign Discourse on Cyber Conflict Under International Law, Texas Law Review (2010). Disponível em: . Acesso: em 20 jul. 2016.

LIVRO BRANCO DE DEFESA. Disponível em: file:///C:/Users/Windows%207/Downloads/lbdn.pdf Acesso em 17 mai. 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Reports of International Arbitral Awards: Islands of Palmas case. Corte Permanente de Arbitragem (1928). Disponível em: . Acesso em: 05 jul. 2016.

SCHMITT, Michael. The Law of Cyber Warfare: Quo Vadis, Stanford Law & Policy Review (2014) Disponível em: . Acesso em: 17 de jul. 2016.

THE WHITE HOUSE. International Strategy for Cyberspace. White House (2011). Disponível em: . Acesso em: 15 jul. 2016.

WEDGWOOD, Ruth. Proportionality, Cyberwar, and the Law of War, U.S. Naval War College International Law Studies (2002). Disponível em: . Acesso em: 21 de jul. 2016.